WEOS-16-03: Security Advisory

CRITICAL / HIGH / MEDIUM / LOW 2016-02-19

Description

Westermo is working on a permanent fix for a vulnerability reported in CVE-2015-7547 and recommended short term mitigation can be found in the ***Mitigation*** section of this advisory.

An attacker that successfully masquerade as an upstream DNS server may serve the WeOS device with malicious DNS query response that can allow the attacker full unauthorized access to the device.

"The glibc DNS client side resolver is vulnerable to a stack-based buffer overflow when the getaddrinfo() library function is used. Software using this function may be exploited with attacker-controlled domain names, attacker-controlled DNS servers, or through a man-in-the-middle attack."

Affected versions

Westermo products running any of the following the WeOS operating system versions are susceptible to this vulnerability:

4.12.0 to 4.18.0

Impact

All services in WeOS that query DNS are potentially vulnerable.

Severity

The CVSS[1] severity base score is 10.0,
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Mitigation

The vulnerability can be mitigated by configuring the DNS servers to be 127.0.0.1 and add static hostname lookup entries using the CLI for all hostnames configured in the device, for example RADIUS, NTP, VPN, etc.

Refer to the WeOS appropriate Management Guide for more information. For WeOS version 4.18.0, relevant sections are:

- 19.3.3 DNS client – setting DNS server and dynamic DNS
- 19.7.8 Add static hostname lookup entry

[1] For more information on CVSS score, see: https://www.first.org/cvss/calculator/3.0

Updates

An update that permanently fixes this vulnerability is under development.

References

https://googleonlinesecurity.blogspot.se/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html

https://github.com/fjserna/CVE-2015-7547

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7547